ВЕРИФИКАЦИЯ МОДУЛЯРНОГО РАЗДЕЛЕНИЯ СЕКРЕТА

Г.В. Матвеев[1], **Т.В. Галибус**[2]

[1]Белгосуниверситет, факультет прикладной математики и информатики
Независимости 4, 220050 Минск, Беларусь matveev@bsu.by
[2]Белгосуниверситет, факультет прикладной математики и информатики
Независимости 4, 220050 Минск, Беларусь tan2tan@gmail.com

Схемы разделения секрета (СРС) лежат в основе многих криптографических протоколов. В частности, разделение секрета применяется для совместных конфиденциальных вычислений [1], шифрования на основе атрибутов [2] и электронного защищенного голосования [3]. Важной задачей в разделении секрета является построение таких схем, где пользователи могут проверить корректность секрета и тем самым не допустить обман со стороны остальных участников и дилера. В схемах верифицируемого разделения секрета (СВРС) дилер распределяет информацию о секретном значении среди участников таким образом, что для честных пользователей гарантируется получение ими значения секрета, а для нечестных - невозможность восстановить секрет.

СВРС позволяет "честным"пользователям т.е. тем, которые следуют протоколу восстановления секрета, проверить корректность частичных секретов при их распределении и восстановлении исходного секрета. Верификация разделения секрета лежит также в основе криптографического протокола совместных конфиденциальных вычислений (СКВ) [1] .

В основе верификации схем разделения секрета лежит подход Фельдмана [4], который основывается на свойстве гомоморфности функции дискретного логарифма. Позже Беналоу [2] предложил еще один подход. Оба этих метода применяются лишь для верификации параметров пороговой схемы Шамира.

В последние годы получили развитие методы верификации для модулярного разделения секрета, что обусловлено быстродействием модулярного алгоритма восстановления [5], адаптивными свойствами таких схем [6] и возможностью включить верификацию для произвольных структур доступа [7]. Изучением данного вопроса занимались Ифтене [8], Кьонг и др.[9], Кайя и Сельджук [10]. В их работах предложены алгоритмы верификации для модулярных пороговых схем Миньотта [11] и Асмуса-Блюма [5] в кольце целых чисел. Общим недостатком данных методов является их применимость лишь в кольце целых чисел, что, в силу отсутствия совершенной схемы в этом кольце [12] делает их неприменимыми на практике. Преимуществом предложенных нами полиномиальных схем модулярного разделения секрета является их теоретико-информационная стойкость: полиномиальная модулярная схема является, в общем случае, совершенной, а в пороговом - идеальной [7].

Поэтому верификация полиномиальной модулярной схемы является актуальной задачей. Нами предлагается верификация всех параметров разделения секрета, т.е. дилер публикует секретные параметры, включая основной секрет, зашифрованные односторонней функцией верификации.

Пороговая полиномиальная модулярная СРС была предложена в работах [6], [7] и уже принята в качестве стандарта в РБ (СТБ 34.101.60). Данная схема позволяет разделить секретное значение $s(x) \in F_p[x]$. Промежуточный секрет $S(x)$ (t,k)-пороговой модулярной полиномиальной схемы выбирается так, чтобы $degS(x) < tn$, где t - порог, а n - общая степень модулей участников.

Для разделения секрета случайным образом выбирается промежуточное значение секрета $S(x) \in F_p[x]$ с условием $degS(x) < tn$. Случайным образом выбираются попарно различные неприводимые $m_i(x), i = 1,..,k$ и $p(x)$ с ограничением $degm_i(x) = degp(x) = n$. В работе [7] указан способ выбора параметров t, k, n, p. Дилером публикуются $m_i(x), p(x)$, а $s(x) = S(x) \bmod p(x)$ назначается в качестве секрета схемы. Дилером по секретным каналам участников отправляются их частичные секреты: $s_i(x) = S(x) \bmod m_i(x)$.

Для восстановления участники из подмножества A обмениваются своими частичными секретами $s_i(x), i \in A$ и находят значение секрета $s(x)$ применяя алгоритм CRT.

Пусть заданы параметры (t, k)-пороговой модулярной схемы:

$$m_1(x), m_2(x), \ldots, m_k(x), p(x), S(x), s(x) \in F_p[x].$$

При этом, $s(x) = S(x) \bmod p(x)$ или $S(x) = p(x)q(x) + s(x)$. Обобщая известный метод верификации Фельдмана [4], предлагается поступить следующим образом. Пользователю, т.е. обладателю полинома $s_i(x), i = 1, 2, \ldots, k$ фактически необходимо проверить условие: $S(x) = m_i(x)q(x) + s_i(x)$ или $s_i(x) = S(x) \bmod m_i(x)$, при том, что полином S(x) остается скрытым.

С этой целью условие $S(x) = m_i(x)q(x) + s_i(x)$ перепишем в виде: $S(\alpha_j) = s_i(\alpha_j), j = 1, 2, ..., n$, где $\alpha_1, \alpha_2, ..., \alpha_n$ - корни многочлена $m_i(x)$. Это позволяет полиномиальную схему Асмута-Блюма интерпретировать как схему Шамира, а значит, применима верификация по Фельдману [4].

Литература

1. Cramer R., Damgard I., Nielsen J. *Multiparty Computation from Threshold Homomorphic Encryption* // LNCS. 2001. Vol. 2045. P. 280–300.

2. Bethencourt J., Sahai A., Waters B. *Ciphertext-policy attribute-based encryption* // Proceedings of IEEE Symposium on Security and Privacy. 2007. P. 321–334.

3. Benaloh J. *Secret sharing homomorphisms: keeping shares of a secret secret* // LNCS. 1987. Vol. 263. P. 251–260.

4. Feldman P. *A practical scheme for non-interactive verifiable secret sharing* // IEEE Symposium on Foundations of Computer Science. 1987. P. 427–437.

5. Asmuth C. A. , Bloom J. *A modular approach to key safeguarding* // IEEE Transactions on Information Theory. - 1983. - Vol. 29. - P. 156-169.

6. Galibus T. Matveev G. Shenets N. *Some structural and security properties of the modular secret sharing* // Proc. of SYNASC'08, IEEE Comp. soc. press, Los Alamitos, 2009. P. 197-200.

7. Galibus T. Matveev G. *Generalized Mignotte Sequences in Polynomial Rings* // ENTCS. 2007. Vol. 186. P. 39–43.

8. Iftene S. *Secret sharing schemes with applications in security protocols.* Technical Report TR 07-01 // University Alexandru Ioan Cuza of Iasi, Faculty of Computer Science. 2007.

9. Qiong L., Zhifang W., Xiamu N., Shenghe S. *A non-interactive modular verifiable secret sharing scheme* // Proc. of ICCCAS'05, 2005. Vol.1. P. 84–87.

10. Kaya K., Selcuk A. *A Verifiable Secret Sharing Scheme Based on the Chinese Remainder Theorem.* // LNCS. 2008. Vol.5365. P. 288–305.

11. Mignotte M. *How to share a secret* // Advances in cryptology - Eurocrypt'82, LNCS. 1982. P. 371–375.

12. Quisquater M., Preneel B., Vandewalle J. *On the security of the threshold scheme based on the Chinese remainder theorem* // LNCS. 2002. Vol. 2274. P. 199–210.